

UNITED STATES DISTRICT COURT

for the
Southern District of Alabama

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

information associated with Instagram account
"██████████" (account number ██████████) that is
stored at premises controlled by Meta Platforms, Inc.

Case No. MJ-22- 224

Filed under seal

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See Attachment A (incorporated by reference).

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):
See Attachment B (incorporated by reference).

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

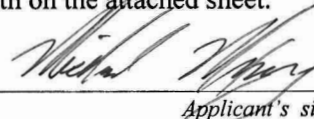
The search is related to a violation of:

Code Section
18 U.S.C. §§ 1349, 1344,
1704, 1708, and 1028A

Offense Description
Fraud conspiracy, bank fraud, stolen or reproduced mail keys or locks, mail theft,
and aggravated identity theft

The application is based on these facts:
See attached affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Michael Maxey, U.S. Postal Inspector

Printed name and title

Sworn to before me and attestation acknowledged pursuant to FRCP 4.1(b)(2).

Date: 12/29/2022

P. Bradley Murray Digitally signed by P. Bradley Murray
Date: 2022.12.29 15:16:07 -06'00'

Judge's signature

City and state: Mobile, Alabama

P. Bradley Murray, U.S. Magistrate Judge

Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ALABAMA
SOUTHERN DIVISION**

**IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
INSTAGRAM ACCOUNT “[REDACTED]”
(ACCOUNT NUMBER [REDACTED] THAT
IS STORED AT PREMISES CONTROLLED
BY META PLATFORMS, INC.**

MJ-22- 224

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Michael Maxey, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Instagram account that is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc. (“Meta”), an electronic communications service and/or remote computing service provider headquartered at 1601 Willow Road in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Meta to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Postal Inspector with the U.S. Postal Inspection Service (“USPIS”) and have been since August 18, 2017. During that time, I have worked on many investigations involving the theft of mail and various postal crimes. Before becoming an Inspector, I attended the Postal

SEALED

Inspector Basic Training in Potomac, Maryland for three months and received training on criminal investigative techniques and practices. Before joining USPIS, I worked over seven years as a police officer in Mobile, Alabama. During that time, I spent over three years as a detective in the Mobile Police Department's ("MPD") Financial Crimes Unit, and I was also a federally deputized taskforce officer for the United States Secret Service where I investigated both federal and state fraud-related crimes. My duties as a Postal Inspector with USPIS include investigating of mail theft, mail fraud, wire fraud, bank fraud, identity theft, and aggravated identity theft, among other crimes. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. All dates, amounts, and locations referenced in my affidavit are approximations.

3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1349 (fraud conspiracy), 1344 (bank fraud), 1704 (stolen or reproduced mail keys or locks), 1708 (mail theft), and 1028A (aggravated identity theft) have been committed by **Johnathan Earl Kyser** ("Kyser"), Delvin Lee Andrews ("Andrews"), Jairice Lynn Shelton ("Shelton"), Arrington Jaylun Gardner ("Gardner"), and others. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, or fruits of these crimes further described in Attachment B.

JURISDICTION

4. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated."

PROBABLE CAUSE

5. Since December 2021, I have been investigating **Kyser**, Shelton, Gardner, Andrews, and several coconspirators for a counterfeit check-cashing scheme (“the scheme”) involving the theft of mail from businesses within the Southern District of Alabama and the use of checks stolen from the mail to produce counterfeit checks, which are then deposited into the accounts of various accountholders who knowingly provide their debit/credit cards and PIN codes to be used in furtherance of the scheme for a share of the illicit proceeds. **Kyser**, Gardner, and 10 other coconspirators were federally indicted for their roles in the scheme in July 2022. *See United States v. Gardner, et al.*, Crim. No. 22-00112-TFM (S.D. Ala.) (“*Gardner*”). On December 5, 2022, **Kyser** pleaded guilty to a charge of conspiracy to commit bank fraud. *Id.*, Doc. 280. Gardner and every other coconspirator in criminal case number 22-00112-TFM also pleaded guilty.

6. In December 2022, a federal grand jury returned a sealed indictment of Shelton, Andrews, and others for, among other things, their participation in and execution of the scheme. *See United States v. Shelton, et al.*, Crim No. 22-00237-TFM (S.D. Ala.) (sealed).

7. On December 9, 2022, U.S. Magistrate Judge P. Bradley Murray signed a federal search warrant for the contents of Andrews’s Instagram account “[REDACTED]” (*see* [REDACTED]). For purposes of brevity, my affidavit fully incorporates the facts from the affidavit that I submitted in support of that search warrant. The results of that search warrant revealed dozens of messages between Andrews and others discussing the scheme and messages exchanged in furtherance of the scheme. As discussed further below, I believe that the results of that search warrant and other

information described below provide probable cause for a search warrant to obtain the communications from **Kyser**'s Instagram account, "[REDACTED]," requested herein.

8. Specifically, I discovered private messages exchanged between Andrews and **Kyser**, using Instagram account "[REDACTED]," in furtherance of the scheme. On July 12, 2022, **Kyser** was arrested and made his initial appearance in criminal case number 22-00112-TFM. The Court released **Kyser** on conditions that ordered him, among other things, not to "commit any offense in violation of federal, state or local law while on release in this action" and to "avoid all contact, directly or indirectly, with any persons who are or who may become a victim [or] potential witness in the subject investigation or prosecution, including, but not limited to: Codefendants." *Gardner*, Doc. 110, PageID.376–77. Four days later, on July 16, 2022, **Kyser** messaged Andrews on Instagram and asked Andrews for his phone number. Andrews provided his cell phone number to **Kyser**. The next day, on July 17, 2022, **Kyser** messaged Andrews and stated, "Post this tell them folks tap in." Andrews replied, "Hell naw them folks watching" (*see* Figure 1 below). Throughout the course of my investigation, I have learned the phrase "tap in" is a phrase used when the individuals involved in the scheme solicit others to join the scheme by providing their account information, debit cards, and PIN codes to allow counterfeit checks to be deposited.

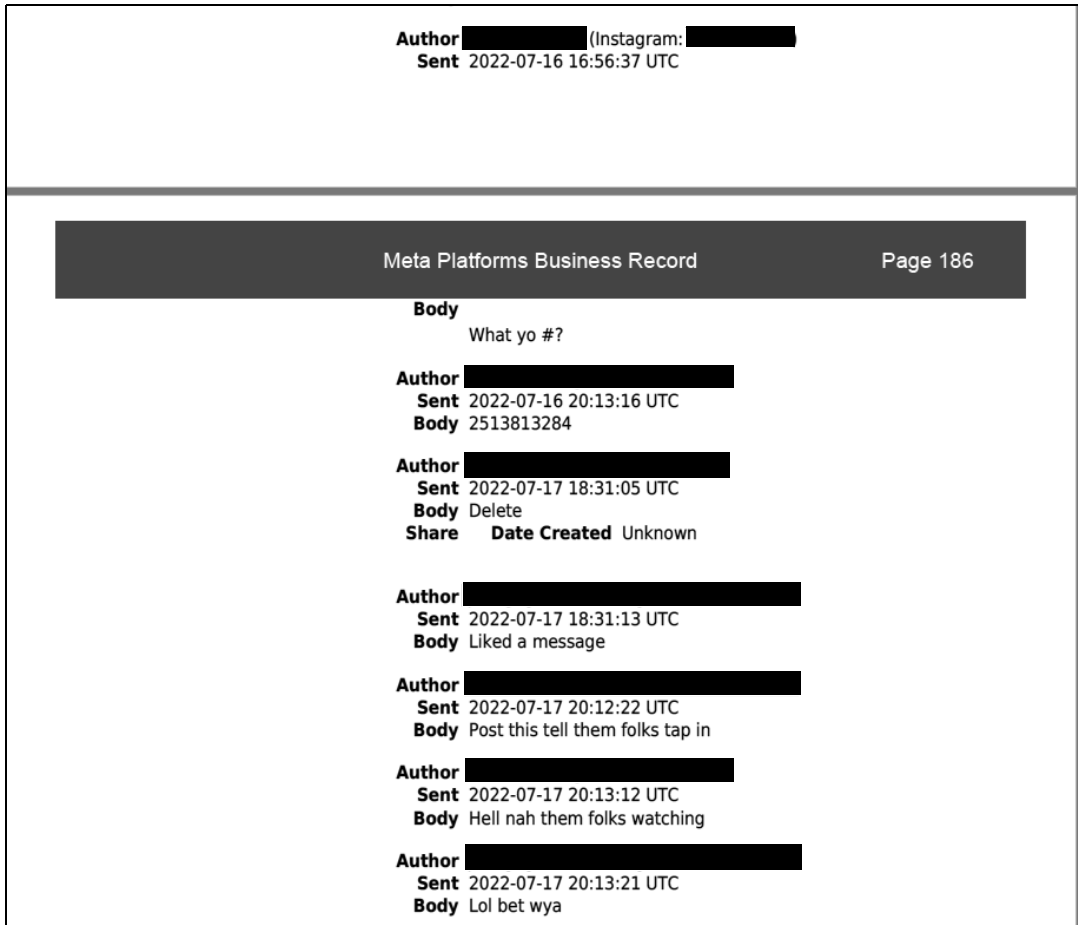



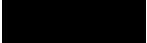
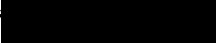
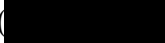
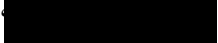
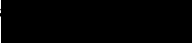
Fig. 1 (Instagram messages between Kyser and Andrews).

9. On November 10, 2022, U.S. Magistrate Judge Katherine P. Nelson signed additional federal search warrants for the contents of **Shelton’s** Instagram account “**[REDACTED]**” (*see [REDACTED]*). For purposes of brevity, my affidavit fully incorporates the facts from the affidavit that I submitted in support of that search warrant. The results of that search warrant revealed hundreds of messages between Shelton, **Kyser**, and others discussing the scheme and messages exchanged in furtherance of the scheme.

10. Specifically, **Kyser** messaged Shelton on July 14, 2022—two days after **Kyser’s** initial appearance in criminal case number 22-00112-TFM—asking Shelton for his phone number.

11. Since his arrest on July 12, 2022, Gardner has been held in the custody of the United States Marshals Service at the Clarke County Jail. During his time in custody, Gardner has used law enforcement-monitored voice and text-based communications to communicate with Shelton, Andrews, and others. While listening to a conversation between Gardner and Shelton, I observed Shelton inform Gardner that **Kyser** was actively attempting to further the scheme after his arrest and pretrial release. Shelton told Gardner he did not trust **Kyser**, so he did not get involved with **Kyser**.

12. On July 19, 2022, U.S. Magistrate Judge Katherine P. Nelson signed federal search warrants for the contents of Gardner's cellular phones and electronic devices, which law enforcement seized during a residential search warrant executed after Gardner's arrest (*see Gardner*, Docs. 170–87). For purposes of brevity, my affidavit fully incorporates the facts from the affidavit that I submitted in support of those search warrants. The results of those search warrants revealed hundreds of messages between Gardner, **Kyser**, and others discussing the scheme and messages exchanged in furtherance of the scheme.

13. Specifically, Gardner and **Kyser** messaged each other on March 17, 2022, to further the scheme. **Kyser** used his Instagram account, which at the time used the vanity name “ ,” to inform Gardner that he had acquired two more account holders to participate in the scheme (*see* Figure 2 below). I am certain that the “” account is the same account for which I am seeking a warrant the account number () for both the “” account and the “” account is the same (*see* Figure 3 below).

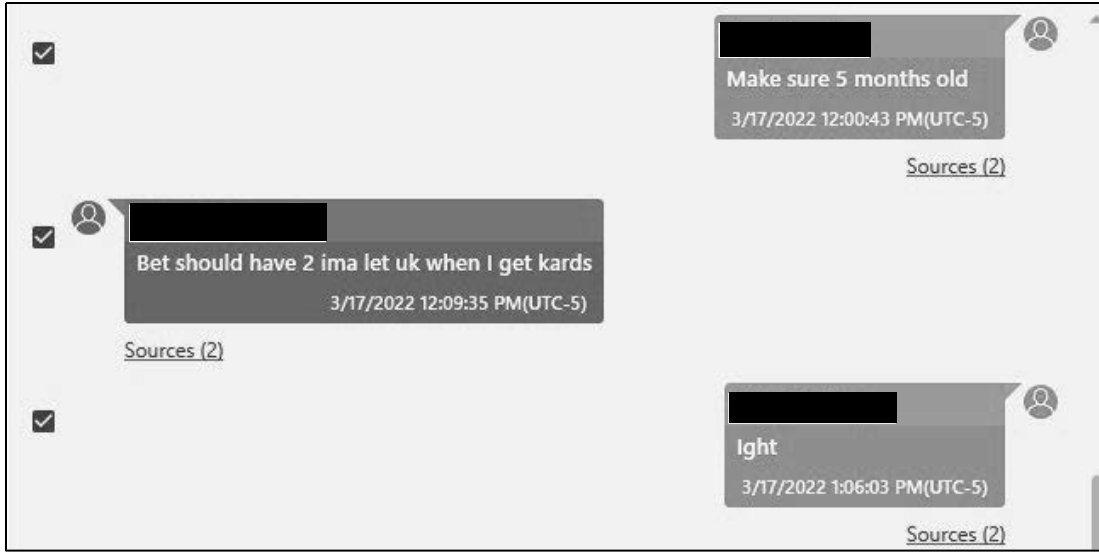


Fig. 2 (Instagram messages between Kyser and Gardner).



Fig. 3 (Kyser's (" ") and Gardner's (" ") Instagram account numbers).

14. In sum, based on the above-referenced facts, I have probable cause to believe that **Kyser** used his Instagram account " " to attempt to facilitate the above-referenced fraud scheme *after* his arrest and initial appearance in criminal case number 22-00112-TFM. **Kyser**, who pleaded guilty and is awaiting sentencing on February 9, 2023 (*Gardner*, Doc. 280), is directly linked with crimes involving Gardner, Shelton, and others dating to at least December 2021 and continuing through July 2022. Based on the information set forth in this

affidavit, I believe probable cause exists to obtain **Kyser's** Instagram content from the account "[REDACTED]" from December 1, 2021, through the present.

BACKGROUND CONCERNING INSTAGRAM¹

15. Instagram is a service owned by Meta, a United States company and a provider of an electronic communications service as defined by 18 U.S.C. §§ 3127(1) and 2510. Specifically, Instagram is a free-access social networking service, accessible through its website and its mobile application, that allows subscribers to acquire and use Instagram accounts, like the target account(s) listed in Attachment A, through which users can share messages, multimedia, and other information with other Instagram users and the general public.

16. Meta collects basic contact and personal identifying information from users during the Instagram registration process. This information, which can later be changed by the user, may include the user's full name, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, credit card or bank account number, and other personal identifiers. Meta keeps records of changes made to this information.

17. Meta also collects and retains information about how each user accesses and uses Instagram. This includes information about the Internet Protocol ("IP") addresses used to create and use an account, unique identifiers and other information about devices and web browsers used to access an account, and session times and durations.

¹ The information in this section is based on information published by Meta on its Instagram website, including, but not limited to, the following webpages: "Privacy Policy," <https://privacycenter.instagram.com/policy/>; "Information for Law Enforcement," <https://help.instagram.com/494561080557017>; and "Help Center," <https://help.instagram.com>.

18. Each Instagram account is identified by a unique username chosen by the user. Users can change their usernames whenever they choose but no two users can have the same usernames at the same time. Instagram users can create multiple accounts and, if “added” to the primary account, can switch between the associated accounts on a device without having to repeatedly log-in and log-out.

19. Instagram users can also connect their Instagram and Facebook accounts to utilize certain cross-platform features, and multiple Instagram accounts can be connected to a single Facebook account. Instagram accounts can also be connected to certain third-party websites and mobile apps for similar functionality. For example, an Instagram user can “tweet” an image uploaded to Instagram to a connected Twitter account or post it to a connected Facebook account, or transfer an image from Instagram to a connected image printing service. Meta maintains records of changed Instagram usernames, associated Instagram accounts, and previous and current connections with accounts on Meta and third-party websites and mobile apps.

20. Instagram users can “follow” other users to receive updates about their posts and to gain access that might otherwise be restricted by privacy settings (for example, users can choose whether their posts are visible to anyone or only to their followers). Users can also “block” other users from viewing their posts and searching for their account, “mute” users to avoid seeing their posts, and “restrict” users to hide certain activity and prescreen their comments. Instagram also allows users to create a “close friends list” for targeting certain communications and activities to a subset of followers.

21. Users have several ways to search for friends and associates to follow on Instagram, such as by allowing Meta to access the contact lists on their devices to identify which contacts are

Instagram users. Meta retains this contact data unless deleted by the user and periodically syncs with the user's devices to capture changes and additions. Users can similarly allow Meta to search an associated Facebook account for friends who are also Instagram users. Users can also manually search for friends or associates.

22. Each Instagram user has a profile page where certain content they create and share ("posts") can be viewed either by the general public or only the user's followers, depending on privacy settings. Users can customize their profile by adding their name, a photo, a short biography ("Bio"), and a website address.

23. One of Instagram's primary features is the ability to create, edit, share, and interact with photos and short videos. Users can upload photos or videos taken with or stored on their devices, to which they can apply filters and other visual effects, add a caption, enter the usernames of other users ("tag"), or add a location. These appear as posts on the user's profile. Users can remove posts from their profiles by deleting or archiving them. Archived posts can be reposted because, unlike deleted posts, they remain on Meta's servers.

24. Users can interact with posts by liking them, adding or replying to comments, or sharing them within or outside of Instagram. Users receive notification when they are tagged in a post by its creator or mentioned in a comment (users can "mention" others by adding their username to a comment followed by "@"). An Instagram post created by one user may appear on the profiles or feeds of other users depending on a number of factors, including privacy settings and which users were tagged or mentioned.

25. An Instagram "story" is similar to a post but can be viewed by other users for only 24 hours. Stories are automatically saved to the creator's "Stories Archive" and remain on Meta's

servers unless manually deleted. The usernames of those who viewed a story are visible to the story's creator until 48 hours after the story was posted.

26. Instagram allows users to broadcast live video from their profiles. Viewers can like and add comments to the video while it is live, but the video and any user interactions are removed from Instagram upon completion unless the creator chooses to send the video to IGTV, Instagram's long-form video app.

27. Instagram Direct, Instagram's messaging service, allows users to send private messages to select individuals or groups. These messages may include text, photos, videos, posts, videos, profiles, and other information. Participants to a group conversation can name the group and send invitations to others to join. Instagram users can send individual or group messages with "disappearing" photos or videos that can only be viewed by recipients once or twice, depending on settings. Senders can't view their disappearing messages after they are sent but do have access to each message's status, which indicates whether it was delivered, opened, or replayed, and if the recipient took a screenshot. Instagram Direct also enables users to video chat with each other directly or in groups.

28. Instagram offers services such as Instagram Checkout and Facebook Pay for users to make purchases, donate money, and conduct other financial transactions within the Instagram platform as well as on Facebook and other associated websites and apps. Instagram collects and retains payment information, billing records, and transactional and other information when these services are utilized.

29. Instagram has a search function which allows users to search for accounts by username, user activity by location, and user activity by hashtag. Hashtags, which are topical

words or phrases preceded by a hash sign (#), can be added to posts to make them more easily searchable and can be “followed” to generate related updates from Instagram. Meta retains records of a user’s search history and followed hashtags.

30. Meta collects and retains location information relating to the use of an Instagram account, including user-entered location tags and location information used by Meta to personalize and target advertisements.

31. Meta uses information it gathers from its platforms and other sources about the demographics, interests, actions, and connections of its users to select and personalize ads, offers, and other sponsored content. Meta maintains related records for Instagram users, including information about their perceived ad topic preferences, interactions with ads, and advertising identifiers. This data can provide insights into a user’s identity and activities, and it can also reveal potential sources of additional evidence.

32. In some cases, Instagram users may communicate directly with Meta about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user as a result of the communications.

33. For each Instagram user, Meta collects and retains the content and other records described above, sometimes even after it is changed by the user (including usernames, phone numbers, email addresses, full names, privacy settings, email addresses, and profile bios and links).

34. In my training and experience, evidence of who was using Instagram and from where, and evidence related to criminal activity of the kind described above, may be found in the

files and records described above. This evidence may establish the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

35. For example, the stored communications and files connected to an Instagram account may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, voice messages, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

36. In addition, the user’s account activity, logs, stored electronic communications, and other data retained by Meta can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, messaging logs, photos, and videos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

37. Account activity may also provide relevant insight into the account owner’s state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan

to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

38. Other information connected to the use of Instagram may lead to the discovery of additional evidence. For example, associated and linked accounts, stored communications, photos, and videos may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, stored communications, contact lists, photos, and videos can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

39. Therefore, Meta's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Instagram. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

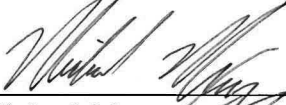
CONCLUSION

40. Based on the forgoing, I request that the Court issue the proposed search warrant.

41. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Meta. Because the warrant will be served on Meta, who will then compile

the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



Michael Maxey
Postal Inspector
U.S. Postal Inspection Service

THE ABOVE AGENT HAS ATTESTED
TO THIS AFFIDAVIT PURSUANT TO
FED. R. CRIM. P. 4.1(b)(2)(B) THIS 29th
DAY OF DECEMBER 2022.

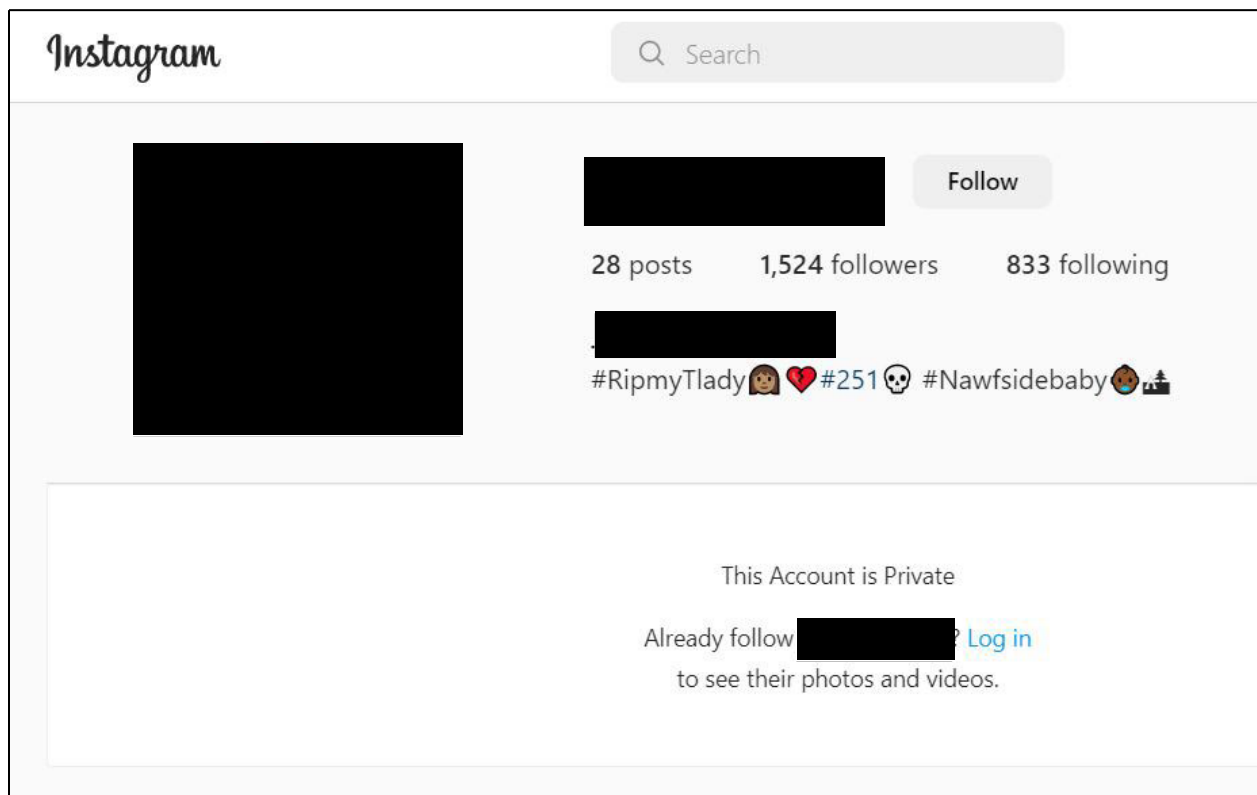
P. Bradley Murray Digitally signed by P. Bradley Murray
Date: 2022.12.29 15:23:06 -06'00'

P. BRADLEY MURRAY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Instagram account “[REDACTED]” (account number [REDACTED] (active on, but not limited to, December 26, 2022), that is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc., a company headquartered at 1601 Willow Road, Menlo Park, California. A screenshot of the public-facing page for the account appears below.



SEALED

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, Inc. (“Meta”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or other information that has been deleted but is still available to Meta, Meta is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- A. All business records and subscriber information, in any form kept, pertaining to the account, including:
1. Identity and contact information (past and current), including full name, e-mail addresses, physical address, date of birth, phone numbers, gender, hometown, occupation, websites, and other personal identifiers;
 2. All Instagram usernames (past and current) and the date and time each username was active, all associated Instagram and Facebook accounts (including those linked by machine cookie), and all records or other information about connections with Facebook, third-party websites, and mobile apps (whether active, expired, or removed);
 3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;

SEALED

4. Devices used to login to or access the account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;
 5. All advertising information, including advertising IDs, ad activity, and ad topic preferences;
 6. Internet Protocol (“IP”) addresses used to create, login, and use the account, including associated dates, times, and port numbers, **from December 1, 2021, through the present;**
 7. Privacy and account settings, including change history; and
 8. Communications between Meta and any person regarding the account, including contacts with support services and records of actions taken;
- B. All content (whether created, uploaded, or shared by or with the account), records, and other information relating to videos (including live videos and videos on IGTV), images, stories and archived stories, past and current bios and profiles, posts and archived posts, captions, tags, nametags, comments, mentions, likes, follows, followed hashtags, shares, invitations, and all associated logs and metadata, **from December 1, 2021, through the present;**
- C. All content, records, and other information relating to communications sent from or received by the account **from December 1, 2021, through the present,** including but not limited to:

1. The content of all communications sent from or received by the account, including direct and group messages, and all associated multimedia and metadata, including deleted and draft content if available;
 2. All records and other information about direct, group, and disappearing messages sent from or received by the account, including dates and times, methods, sources and destinations (including usernames and account numbers), and status (such as delivered, opened, replayed, screenshot);
 3. All records and other information about group conversations and video chats, including dates and times, durations, invitations, and participants (including usernames, account numbers, and date and time of entry and exit); and
 4. All associated logs and metadata;
- D. All content, records, and other information relating to all other interactions between the account and other Instagram users **from December 1, 2021, through the present**, including but not limited to:
1. Interactions by other Instagram users with the account or its content, including posts, comments, likes, tags, follows (including unfollows, approved and denied follow requests, and blocks and unblocks), shares, invitations, and mentions;
 2. All users the account has followed (including the close friends list), unfollowed, blocked, unblocked, muted, restricted, or denied a request to

follow, and of users who have followed, unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow the account;

3. All contacts and related sync information; and
 4. All associated logs and metadata;
- E. All records of searches performed by the account **from December 1, 2021, through the present**; and
- F. All location information, including location history, login activity, information geotags, and related metadata **from December 1, 2021, through the present**.

Meta is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. §§ 1349, 1344, 1704, 1708, and 1028A, those violations involving **Johnathan Earl Kyser** (“**Kyser**”), Delvin Lee Andrews, Jairice Lynn Shelton, Arrington Jaylun Gardner and any coconspirators, and occurring after December 1, 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- A. Evidence of the stealing of mail, the stealing or selling of post office keys, the manufacturing of counterfeit checks, the depositing of counterfeit checks, the solicitation of individuals with accounts at financial institutions in furtherance of counterfeit check cashing, preparatory steps taken in furtherance of the scheme, money laundering, wire fraud, bank fraud, and aggravated identity theft;
- B. Evidence of **Kyser**’s violation of conditions of release in *United States v. Gardner, et al.*, No. 22-cr-00112-TFM (S.D. Ala.);
- C. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;
- D. Evidence indicating the account owner’s state of mind as it relates to the crime under investigation; and
- E. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s).